PATENT COOPERATION TREATY



# PCT

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)



| Applicant's or agent's file reference | FOR FURTHER ACTION | See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416) |
|---|---|---|
| 106040/KR | | |

| International application No. | International filing date *(day/month/year)* | Priority date *(day/month/year)* |
|---|---|---|
| PCT/NO 02/00174 | 15.05.2002 | 22.02.2002 |

International Patent Classification (IPC) or both national classification and IPC
G07F7/08

Applicant
HANDCASH AS et al

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 11 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the opinion
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

| Date of submission of the demand | Date of completion of this report |
|---|---|
| 22.08.2003 | 27.04.2004 |

Name and mailing address of the international preliminary examining authority:

European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized Officer

Rother, S

Telephone No. +49 89 2399-2250

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/NO 02/00174

## I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:

**Description, Pages**

1-8 filed with telefax on 15.04.2004

**Claims, Numbers**

1-15 filed with telefax on 15.04.2004

**Drawings, Sheets**

1/7-7/7 as published

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).

   ☐ the language of publication of the international application (under Rule 48.3(b)).

   ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   ☐ contained in the international application in written form.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority in written form.

   ☐ furnished subsequently to this Authority in computer readable form.

   ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   ☐ the description, pages:

   ☐ the claims, Nos.:

   ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

   *(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)*

6. Additional observations, if necessary:

**V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

| | | | |
|---|---|---|---|
| Novelty (N) | Yes: | Claims | 1,9 |
| | No: | Claims | |
| Inventive step (IS) | Yes: | Claims | |
| | No: | Claims | 1,9 |
| Industrial applicability (IA) | Yes: | Claims | 1,9 |
| | No: | Claims | |

2. Citations and explanations

   **see separate sheet**

Re Item V

**Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. **With telefax of 15.04.2004, the applicant supplied a modification of originally filed independent claims 1 and 9 and a revised description. Having regard to those independent claims, the objections raised in the first communication are being maintained (see written opinion 408 dated 16.12.2003).**

2. Independent claim 1:

Document D2 (EP 1 100 056 A) which is still considered to represent the most relevant state of the art. As already mentioned in the 408-communication, it discloses a method for payment of goods, services and content by using a prepaid card (paragraph [1]), where the card comprises a concealed code (claims 5, 7, 8) and an activation code (claim 2), the method comprising to activate the card at a point of sale for such cards by reading the activation code in a card reader at the point of sale (claim 2, paragraph [19]), whereby [only] the activation code is transmitted to an offeror of the prepaid card together with an ID for the point of sale (c.5, l.7-10; claim 6), and when paying for goods/services from a service provider, to transmit [only] the concealed code together with an ID for the service provider to the card offeror, thereby to cause purchase of the goods/service (claims 4, 8, paragraph [22]).

The applicant has added the word "only" (and has made some further corrections) in order to distinguish claim from D2. The applicant states in the aforementioned letter of reply that other codes (password, reservation number) are send to the card offerer additionally, whereas the application uses only the activation code (card activation process) and only the concealed code (payment process), respectively, and thus the user makes less inputs to activate/use the card.

However, the method according to claim 1 differs from that known from document D2 only in that the feature of using further codes (password, reservation number) has been omitted. Apart from the obviously and consequently simpler design of the method, the only result of this omission is that additional security features as disclosed in D2 are no longer present in the method according to claim 1. Such a simplification does not involve an inventive step (Article 33(3) PCT), because the person skilled in the art would implement less codes in the method to solve the problem of how to provide a simple card payment system.

3. Independent claim 9:

The solution proposed in independent claim 9 of the present application cannot be considered as involving an inventive step (Article 33(3) PCT) because similar objections apply as referred to in respect of independent claim 1 of the application because independent system claim 9 is the direct equivalence of an apparatus of the method defined in independent method claim 1. Having regard to the amendments with telefax of 15.04.2004, the examiner is of the opinion that no essential technical feature have been added, only the principal technical network structure of the system has been claimed in more detail. Features as "at least one electronic commodity/service provider attached to the card offeror by agreement" introduce only administrative subject-matter with no technical relation to the other claimed features.

4. Furthermore, it should be mentioned that the applicant speaks about subject-matter in aforementioned telefax of reply that has no basis in the application as originally filed, e.g. p. 2, paragraph in the middle ("to explain the method steps further..."): Features as "re-direction to the card offerer's system", "icons", "window appears", "send button" etc. do not fulfill Art. 34(2)(b) PCT go beyond the application as originally filed and thus cannot be taken into consideration.

5. Even D1 is still considered as possible closest prior art document because it also comprises an activation code. WIth regard to the more detailed technical infrastructure of code-pairs etc., equivalent objections apply as mentioned before.

# PAYMENT CARD AND PERTAINING METHOD

## INTRODUCTION

The invention concerns a method and a system for prepayment of online goods and services by using a prepaid card. Especially, the invention concerns a system for secure payment of goods, services and content on Internet.

## BACKGROUND

Today there exist payment solutions for goods and services which are sold through web sites. The web sites can charge for goods/services through the mobile phone to a user, through a credit card (e.g. Euro card, American Express) or registered payment cards (e.g. Visa) or in that the user has connected to an IPP (Internet Payment Provider) where the user must register and on his own arrange for filling up the account. Many users have today also a threshold for shopping on the Internet, as they feel a risk by providing their payment card number and personal information on the Internet and many dare therefore not shop with their credit cards in fear of being swindled. By using a payment solution where the customer may put small shopping on his/her cell phone bill, it is also a problem that the cell phone bill shall be paid by others, e.g. an employer, which then shall not be charged for the user's Internet shopping. By opening an account at an IPP the user must also provide personal information. In today's system it is also expensive for the web sites to charge for simple services which shall only cost small amounts (e.g. 10 NOK).

Accordingly there exists a need for a payment solution to be able to charge for goods, services and content in a simple and cheap way for both online service providers and customers, and where the customer may keep his/her anonymity and avoid thorough registering to be able to buy commercial goods or services.

## SUMMARY OF THE INVENTION

The present invention offers a solution to the problem stated above by providing in a first aspect a method for payment of goods, services and content by use of a prepaid card where the card comprises a concealed code and an activation code. The card is activated at a point of sale of the card by reading the activation code in a card reader at the point of sale. Only the activation code is transmitted to an offeror of the prepaid card together with an ID for the point of sale, and

when the card is used for payment of goods/services from a service provider, only the concealed code is transmitted together with an ID for the service provider to the card provider, thereby to cause purchase of the goods/service.

The invention provides also, in another aspect, a system for prepayment of commodities, services and content, the system comprising

- a cash value card prepared by a card offeror and representing a certain money value, the card comprising an activation code and a concealed code,
- a card reader at a point of sale for such cards, for reading only the activation code from the card as part of a transaction with a sale of the card to a user,
- a central computer and data base system belonging to or representing the card offeror, for receiving from the point of sale the activation code and an ID for the point of sale,
- at least one electronic commodity/service provider attached to the card offeror by agreement, and
- a user's computer terminal attached to a network to which the central computer and data base system and the electronic commodity/service providers are also attached, the terminal being used for transmitting only the concealed code together with an ID for an electronic commodity/service provider with whom a transaction is desirable, and the user's choice of commodity/service, to the central computer and data base system, thereby to cause payment for the commodity/service to this electronic commodity/service provider.

The activation of the card preferably takes place in that the activation code is a bar code and that the card is read in a bar code reader. Activation causes that an account opens for the buyer of the card at the card offeror, with an amount corresponding to the prepaid amount. The concealed code can be covered by a thin opaque layer which must be scratched off by a buyer of the card. When the card is used as a payment means, the card offeror checks that the card has been activated, authenticates the concealed code and the service provider ID, and checks that the balance of the account is greater than or equal to the cost of the purchase of the service, before purchase of the service can take place. This control and authentication preferably take place by query against the database of the card offeror, stored on a database server communicating with the transaction server.

In a preferred embodiment, the IP-address of the service provider and at least one unique password are used as the service provider ID. In another embodiment, the ID of the point of sale may however be the phone number of the point of sale and a unique password for the point of sale. The point of sale communicates then with the central systems through the telephone network and/or Internet. The central systems comprise in a preferred embodiment a transaction server which has stored thereon functions for logic and procedures, and a database server comprising a database with data for the prepaid cards, points of sales and service providers, and a firewall between the transaction server and the database server, and where queries against the database are controlled by the transaction server. The database comprises further a table stored for each card, where each table comprises the concealed code, the activation code, whether the card is activated and the balance of the account pertaining to the card, and a table of points of sales and service providers with pertaining IDs. The invention is defined in the appended patent claims.

The payment solution as stated above provides a secure and simple solution with possibility for anonymity for the purchaser of the card and thereby the purchaser of goods/services on electronic sites/interactive trading sites. The trade is settled in cash, which provides cost control for the purchaser when trading in these trading places. For the interactive trading places which are connected to this payment solution, this solution will also provide less loss on debts, and the possibility of charging the customer in advance. Such a payment solution where the customer does not need to use a credit card or other payment card connected to an ordinary bank account, would probably also contribute to expanding the existing market for the trading place.

The security is also taken care of by the number of codes and passwords for the different actors in this payment solution. Each card has a unique activation code and a concealed code which the user uses for payment of goods/services/content. Also the ID of the point of sale and the password for the point of sale. And at last, each web site wanting that the customers shall be able to use this payment solution, has its unique password which is automatically updated on a regular basis, usually every day. The payment solution also demands information on the IP of the web site and IP of the user, if the web site and the user are connected to Internet.

## SHORT DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will now be described with reference to the following drawings, where:

Figure 1A-1C shows a payment card according to an embodiment of the invention;

Figure 2 shows a concept sketch regarding the payment solution according to an embodiment of the invention;

Figure 3 is a flow chart for activation of the payment card in Figures 1A-1C for use in the payment solution in Figure 2 according to an embodiment of the invention;

Figure 4 is a flow chart showing an online payment process by the use of the payment card according to an embodiment of the invention;

Figure 5 is a draft showing cash flow in the payment system according to an embodiment of the invention;

Figure 6 shows a view of the payment system according to an embodiment of the invention where the different actors are connected to Internet; and

Figure 7 shows a view of tables in the database according to an embodiment of the invention.

## DETAILED DESCRIPTION OF THE INVENTION

Figures 1A-1C show an embodiment of a prepaid card. The card has assigned a value (not shown) corresponding to the amount a purchaser must pay for the card. The amount may vary from 50 kroner to several thousand kroner. On the card there is applied a unique activation code, which in Figure 1C is a bar code on the backside of the card, but this unique activation code may also be e.g. a magnetic stripe. The activation code is used when activating the card at a point of sale for the card, by reading the code in a suitable card reader, e.g. a bar code reader or a magnetic card reader. This will be further explained later. In addition there is a hidden code on the card, which code in Figure 1A is hidden under "scraping field". In Figure 1A this area is coated with an opaque coating or film which must be scraped away by the purchaser before the concealed code appears. An example of such a code is shown in Figure 1B, where the code is 1234 5678 EFGH. There is also space for advertisements on the card, e.g. for places of card purchase and for

web sites on Internet where the card can be used as a payment means. The activation code may also be arranged on the front side of the card. An alternative to an activation code is also that the card comes preactivated to the point of sale. This can be an alternative for points of sale which do not have an online card reader. Points of sale can be e.g. kiosks, petrol stations and grocery shops.

The concealed code on the card represents a password which the buyer of the card must use when buying goods and services online at service offerors which are connected to this form of payment. This may be e.g. online newspapers, pools, online trading places, online ticket booking etc. The password is associated with the card, and the card with belonging password can be used several times until the whole amount on the card has been spent. If one is to shop more, one must buy a new card. It is also possible to use several cards in a transaction if the goods or services cost more than the amount which is printed on the card or which remains on the account belonging to the card.

The concept for the trade solution is sketched in Figure 2. In Figure 2 a card with a bar code is used. Other solutions can, as mentioned, above also be used. An approved point of sale for the prepaid paying cards sells the card to a purchaser. The card must thereafter be activated, and this is done by reading of the card in the bar code reader at the point of sale. The unique bar code together with the ID of the point of sale are transmitted to the central system of the card offeror for verification. Only registered point of sales may distribute the prepaid paying cards. Each point of sale is therefore registered in a central database at the card offeror, together with information concerning the identity of the point of sale, i.e. ID. ID may be the telephone number of the point of sale or the IP-address of the point of sale and an assigned password for the point of sale. This activation procedure is shown as a flow chart in Figure 3.

The central system in the payment system comprises a transaction server and a database server which are shown in the system sketched in Figure 6. Between the transaction server and the database server there is, as shown, a firewall for securing the information existing in the database. The transaction server controls all the necessary procedures in the system and performs logic control of the information which is transmitted from points of sales and service providers by communicating with the database. If the ID of the point of sale and the activation code

exist in the database, the card is opened for use and a virtual account is created on the database server. The account is open for trade until the whole amount has been spent.

An overview over the different tables which may exist in the database stored on the database server is shown in Figure 7. The database has a table over the cards, where each entry in the table among other things comprises information concerning the concealed code, the activation code, whether the card has been activated and when, and the balance of the account pertaining to the card. There also exists a table with necessary information about points of sales and service providers (among other things name, address, telephone number) with belonging ID and password. Information about transactions (among other things used ID, product, time, amount, trading place) and the number of cards involved in transactions are also stored. This information may be used in the settlement with the trading places and are also stored in time as a security for the actors involved.

The card can also be used for payment of goods and services when shopping on e.g. the Internet. An example of a payment solution is shown in Figure 4. When a user of the card is to pay for a commodity or service on a web site on Internet, the user only needs to quote the concealed code which has been obtained from the card, along with the commodity/service he has chosen. This information will then be transmitted to the card offeror's central system for verification. In addition to the code information concerning the IP-address of the user, the IP-address of the web site and password are also transmitted. If the password for the web site and the concealed code arrive together with a valid IP for the web site to the transaction server, and the card is registered as activated and the balance of the card is greater than a desired amount, there will be performed an adjustment of the balance for this card in the database stored on the database server, corresponding to the amount which the customer shall pay for the commodity/service desired from the web site. If the balance is not adequate to pay for the commodity/service, the user receives a message that a new card can be used. In this way several cards can be used together to pay for a commodity/service. If a user of the card provides the wrong code more than three times, this user's IP will be closed for use. The card will be closed for use if there occur errors in one of the passwords or other necessary information more than twice.

A password for a trading place is generated every day by the transaction server in the central system of the card offeror, stored in the database on the database server, and entered into the trading place systems automatically without the trading place "seeing" this. A trading place can be allocated more than one password, and which password to be used in connection with a payment transaction is then arbitrary. This provides increased security in the system.

The cash flow in this payment system among the different actors is shown in Figure 5. Points of sale for the card buy payment cards from the card offeror and sell the cards to the users of the online trading places. When a user buys a commodity or a service (also includes content) electronically, the transaction is registered in the database at the card offeror. The online trading place where the user has used the card as means of payment for goods/commodity, sends a collective invoice to the card offeror. This invoice is checked against the account information in the database of the card offeror, and which pays out the amount to the online trading places' account. The whole process may take place electronically.

An example of a system for a payment solution with a prepaid card is shown in Figure 6. Here, the different actors in the system are connected via Internet, and all the interfaces in the different systems are then adapted to this. In this case the bar code reader at the point of sale for the card is connected to Internet via a PC. Both analogue and digital connection solutions are possible. The online trading places exist in Figure 6 on Internet, and the user can buy goods and services in these by using a regular PC for home use and the prepaid card. The only thing the user is supposed to do after having chosen the commodity/service, is to state the concealed code on the card to the card offeror's central system. The user's IP-address will be transmitted to the card offeror's central system automatically, together with the other necessary information from the electronic trading place. The transaction server communicates with Internet via a TCP/IP interface. The database server in the central system is protected with an appropriate firewall. The communication which takes place on Internet among the different actors in the system is in encrypted form.

The card may also be used in payment solutions where the user communicates with a service provider via mobile phone (WAP) or another hand held electronic communication device. All the user has to do is to provide the concealed code on the card to the card offeror's system.

# CLAIMS

1. Method for payment of goods, services and content by using a prepaid card, where the card comprises a concealed code and an activation code, the method comprising:

to activate the card at a point of sale for such cards by reading the activation code in a card reader at the point of sale, whereby only the activation code is transmitted to an offeror of the prepaid card together with an ID for the point of sale, and

when paying for goods/services from a service provider, to transmit only the concealed code together with an ID for the service provider to the card offeror, thereby to cause purchase of the goods/service.

2. Method according to claim 1,
characterized in that the activation of the card causes opening of an account for the card at the card offeror, with an amount corresponding to the prepaid amount.

3. Method according to claim 2,
characterized in that the card offeror checks that the card has been activated, authenticates the concealed code and the ID of the service provider, and checks that the balance of the account is larger than or equal to the cost for purchase of the service, before purchase of the service can take place.

4. Method according to claim 3,
characterized in that checking and authenticating take place by query against the card offeror's database stored on a database server communicating with a transaction server.

5. Method according to claim 1,
characterized in that the activation code is a bar code and that the card is read in a bar code reader.

6. Method according to claim 1,
characterized in that the concealed code is covered by a thin opaque layer which must be scraped off by a buyer of the card.

7. Method according to claim 1,
characterized in that the ID of the service provider is an IP-address and at least one unique password.

8. Method according to claim 1,
characterized in that the ID for the point of sale is the phone number of the point of sale and a unique password for the point of sale, and that the point of sale communicates with the card offeror via a telephone network and/or Internet.

9. A system for prepayment of commodities, services and content, the system comprising
- a cash value card prepared by a card offeror and representing a certain money value, said card comprising an activation code and a concealed code,
- a card reader at a point of sale for such cards, for reading only said activation code from said card as part of a transaction with a sale of said card to a user,
- a central computer and data base system belonging to or representing the card offeror, for receiving from said point of sale said activation code and an ID for the point of sale,
- at least one electronic commodity/service provider attached to the card offeror by agreement, and
- a user's computer terminal attached to a network to which said central computer and data base system and said electronic commodity/service providers are also attached, said terminal being used for transmitting only the concealed code together with an ID for an electronic commodity/service provider with whom a transaction is desirable, and the user's choice of commodity/service, to said central computer and data base system, thereby to cause payment for the commodity/service to this electronic commodity/service provider.

10. System according to claim 9,

characterized in that the activation code is a bar code, the card reader is a bar code reader, and the ID for the point of sale is the point of sale's telephone number and a unique password.

11. System according to claim 9, characterized in that the service provider is a web site on Internet and that the ID of the service provider is the IP-address of the web site and at least one unique password for the service provider.

12. System according to claim 11, characterized in that the user communicates with a service provider and the central system via a PC, mobile phone, or another electronic communication device.

13. System according to claim 9, characterized in that the central system comprises a transaction server which has stored thereon functions for logic and procedures, a database server comprising a database with data for prepaid cards, points of sales and service providers, and a firewall between the transaction server and the database server, and where queries against the database are checked by the transaction server.

14. System according to claim 13, characterized in that the database comprises a table of entries for all cards, where a record for each card comprises the concealed code, the activation code, whether the card is activated or not, and the balance of the account belonging to the card, and a table of points of sales and service providers with pertaining IDs.

15. System according to claim 9, characterized in that the card reader is connected to a PC which further is connected to Internet.